Copy to H C S.G

15(L)

GERMAN AND ITALIAN CORRESPONDENCE ON MISCELLANEOUS CYPHERS

Attached is a translation of some extracts from Ticom document T3812, which was among the OKW documents found at Schliersee. It consists of a file of correspondence in German and Italian between OKW/Chi and the Italian Cryptographic Bureau in 1940-41, containing progress reports on the cyphers of various countries, mainly diplomatic.

TICOM

6th March, 1946. No. of pages: 4

DISTRIBUTION

British:

D.D.3.
H.C.G.
D.D.(M.W.)
D.D.(A.S.)
C.C.R.
Cdr. Tandy
Major Morgan

U.S.

Op-20-G (4) (via Cdr. Manson)
G-2 (via Lt. Col. Hilles)
A.S.A. (4) (via Capt. Collins)
Director, A.S.A. Europe
Col. Kunkel, USAAFE

TICOM

S.A.C.
Cdr. Manson
Capt. Collins
Ticom Files (4)

Additional

S.A.C. for H.C.S.G.

11th March, 1941.

Dispatch No. 7.

Herewith:

1) Yugoslavia: Idents for the new diplomatic [code].

2) Greece: Idents for the Greek code "Z".

3) English Air Force: this material is not being worked on here at all. The German Air Force has made several attempts to solve the cypher. The present view is that this cypher is based on a machine. An attempt has also been made to reconstruct such a machine. This work has had no success, however, and the cypher is still not being read.

(Original in German, and apparently addressed to the Italians.)

Rome, 16/8/41-XIX.

Dear Colonel,

Concerning your request of 16th July, regarding the Rumanian cypher which you desire, I have pleasure in informing you that this document will be placed at your disposal.

On 2nd July last I sent you a copy of the Swiss cypher in French reconstructed by us, with 65 keys appended; I hope you have already received it.

I take the opportunity of asking you to supply copies of the following cyphers if they are in your possession:

a) Turkish diplomatic cypher used for communication between Berlin and Ankara;*

b) Turkish military attaché cypher, used between Berlin and Ankara;

c) English diplomatic cypher with figure recyphering tables, used for secret communications, [pencil note: interdepartmental code];

d) Russian diplomatic and field cyphers.

I thank you for and reciprocate, also in the name of my colleagues, your good wishes which you sent us also in the name of your esteemed colleagues.

(signed) Gamba.

Colonel Kempf
Cypher Dept.
OKW, Berlin.

Note: * The recipient subsequently noted opposite these requests: a) Yes, b) c) and d) No.

(Original in Italian).

3/9/41.

Cypher Dept.,
OKW, Section Head.

[Ms. note in German: Copy of draft which was sent to Gamba, as he states he has not received the letter].

Dear General,

I have been away on business for practically the whole of the last few weeks. I have therefore unfortunately been unable to answer all letters and enquiries at once. Please excuse the delay in the circumstances.

I received your dispatch (of 2/7/41) with the Swiss cypher in French, and in my dispatch No. 20 of 22/7/41 I responded with my contribution to the idents and table. This mutual inter-change was very satisfactory.

To the questions in your letter of 16/8/41 and in your Aide Memoire of 24/8/41 I can only give the following replies at present.

The Turk (diplomatic Berlin-Ankara) is being very satisfactorily broken here. Your telegrams of the 24th of August are returned, herewith, completed. In addition, I am enclosing some idents, and more will follow. Since our relative subtractors differ from each other you will have to undertake the small task of conversion. All further details are given in the appendix.

The Turk (military attaché, Berlin-Ankara) is not worked on here because the material is much too thin. For this reason I cannot, unfortunately, offer my co-operation.

The English (with figure subtractor).

I had this cypher worked on months ago but gave up work on it because the employment of about 40 people was out of proportion to the expected result. The subtractor changes frequently and even in the most favourable cases, belated results only were expected. For these reasons I have had nothing further done with this cypher.

Russia.

The diplomatic cyphers have not been worked on for several years because the complicated subtractor recypherments make any success illusory. The army cyphers are so numerous and at times so involved that a description of these cyphers would be useless without detailed explanations. At the moment we have no time for this since all personnel of the Russian decyphering Section are actively employed. If you, Herr General, attach importance to co-operation in Russian Army traffic I request that a specialist be sent. The principal cyphers could be shown to him in about 8 days and the most important could be explained in sufficient detail. The gentleman would need some cryptographic knowledge and a good knowledge of Russian. He would also have to have numerous fellow workers since one person alone is not sufficient to work on all the cyphers received.

Rumania:

I thank you most heartily for the new military attaché [cypher]. Quite apart from the fact that the cypher is extremely complicated it is, also, objectively very interesting and difficult to break. I hope that this cypher will remain in use for 3 or 4 years at least and produce good results.

With comradely greetings to your colleagues, I am

Yours most sincerely,

(Original in German).

Rome

3rd October, 1941 - XIX.

Dear Colonel,

I am sending you copies of the following cyphers:

a) new Turkish military attaché cypher

b) a list of new words for the Turkish cypher T8.

c) American diplomatic cypher A1.

Cypher A1 is used with substitution tables. The tables actually in use are not in our possession but we are now engaged in reconstructing them. I am sending you together with the cypher, copies of the old tables with the necessary instructions for commencing work.

I request you to supply the following material, if it is in your possession:

a) diplomatic cypher of the U.S.A. B1 and C1, recyphered with letter tables.

b) French recyphered diplomatic cypher.

c) Russian diplomatic cypher.

With my sincere good wishes and thanks.

(signed) Gamba.

To Colonel Kempf
Chiffrier Abteilung
Oberkommando der Wehrmacht
Berlin.

(Original in Italian).